

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Assistant Commissioner for Patents
 United States Patent and Trademark
 Office
 Box PCT
 Washington, D.C.20231
 ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 12 August 1999 (12.08.99)	
International application No. PCT/EP99/00283	Applicant's or agent's file reference WO 2585-dV/jdh
International filing date (day/month/year) 14 January 1999 (14.01.99)	Priority date (day/month/year) 14 January 1998 (14.01.98)
Applicant WAJS, Andrew, Augustine	

1. The designated Office is hereby notified of its election made:

☒

in the demand filed with the International Preliminary Examining Authority on:

22 July 1999 (22.07.99)

☐

in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was☐

was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Lazar Joseph Panakal Telephone No.: (41-22) 338.83.38
--	---

E.K.

PATENT COOPERATION TREATY

PCT

NOTIFICATION OF THE RECORDING
OF A CHANGE(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

DE VRIES, Johannes, Hendrik, Fokke
De Vries & Metman B.V.
Overschiestraat 184 N
NL-1062 XK Amsterdam
PAYS-BAS

Date of mailing (day/month/year) 13 October 1999 (13.10.99)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference WO 2585-dV/jdh	
International application No. PCT/EP99/00283	International filing date (day/month/year) 14 January 1999 (14.01.99)

1. The following indications appeared on record concerning:		
<input checked="" type="checkbox"/> the applicant	<input type="checkbox"/> the inventor	<input type="checkbox"/> the agent
<input type="checkbox"/> the common representative		
Name and Address IRDETO B.V. Jupiterstraat 42 NL-2132 HD Hoofddorp Netherlands	State of Nationality NL	State of Residence NL
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	
2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:		
<input type="checkbox"/> the person	<input checked="" type="checkbox"/> the name	<input type="checkbox"/> the address
<input type="checkbox"/> the nationality		
<input type="checkbox"/> the residence		
Name and Address MINDPORT B.V. Jupiterstraat 42 NL-2132 HD Hoofddorp Netherlands	State of Nationality NL	State of Residence NL
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	
3. Further observations, if necessary:		
4. A copy of this notification has been sent to:		
<input checked="" type="checkbox"/> the receiving Office	<input type="checkbox"/> the designated Offices concerned	
<input type="checkbox"/> the International Searching Authority	<input checked="" type="checkbox"/> the elected Offices concerned	
<input checked="" type="checkbox"/> the International Preliminary Examining Authority	<input type="checkbox"/> other:	

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Marie-José Devillard
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PCT COOPERATION TRE/ Y

PCT

NOTIFICATION OF THE RECORDING
OF A CHANGE(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

DE VRIES, Johannes, Hendrik, Fokke
De Vries & Metman B.V.
Overschiestraat 184 N
NL-1062 XK Amsterdam
PAYS-BAS

Date of mailing (day/month/year) 29 February 2000 (29.02.00)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference WO 2585-dV/jdh	
International application No. PCT/EP99/00283	International filing date (day/month/year) 14 January 1999 (14.01.99)

1. The following indications appeared on record concerning:		
<input checked="" type="checkbox"/> the applicant	<input type="checkbox"/> the inventor	<input type="checkbox"/> the agent <input type="checkbox"/> the common representative
Name and Address MINDPORT B.V. Jupiterstraat 42 NL-2132 HD Hoofddorp Netherlands	State of Nationality NL	State of Residence NL
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	
2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:		
<input checked="" type="checkbox"/> the person	<input type="checkbox"/> the name	<input type="checkbox"/> the address <input type="checkbox"/> the nationality <input type="checkbox"/> the residence
Name and Address IRDETO ACCESS B.V. Jupiterstraat 42 NL-2132 HD Hoofddorp Netherlands	State of Nationality NL	State of Residence NL
	Telephone No.	
	Facsimile No.	
	Teleprinter No.	
3. Further observations, if necessary:		
4. A copy of this notification has been sent to:		
<input checked="" type="checkbox"/> the receiving Office	<input type="checkbox"/> the designated Offices concerned	
<input type="checkbox"/> the International Searching Authority	<input checked="" type="checkbox"/> the elected Offices concerned	
<input type="checkbox"/> the International Preliminary Examining Authority	<input type="checkbox"/> other:	

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Marie-José Devillard
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

TENT COOPERATION TRE, Y

PCT

NOTIFICATION OF THE RECORDING
OF A CHANGE(PCT Rule 92bis.1 and
Administrative Instructions, Section 422)

From the INTERNATIONAL BUREAU

To:

DE VRIES, Johannes, Hendrik, Fokke
De Vries & Metman B.V.
Overschiestraat 180
NL-1062 XK Amsterdam
PAYS-BAS

Date of mailing (day/month/year) 20 March 2000 (20.03.00)	IMPORTANT NOTIFICATION
Applicant's or agent's file reference WO 2585-dV/jdh	
International application No. PCT/EP99/00283	International filing date (day/month/year) 14 January 1999 (14.01.99)

1. The following indications appeared on record concerning:		
<input type="checkbox"/> the applicant	<input type="checkbox"/> the inventor	<input checked="" type="checkbox"/> the agent
<input type="checkbox"/> the common representative		
Name and Address DE VRIES, Johannes, Hendrik, Fokke De Vries & Metman B.V. Overschiestraat 184 N NL-1062 XK Amsterdam Netherlands	State of Nationality	State of Residence
	Telephone No. 31 20 669 44 32	
	Facsimile No. 31 20 669 45 16	
	Teleprinter No.	
2. The International Bureau hereby notifies the applicant that the following change has been recorded concerning:		
<input type="checkbox"/> the person	<input type="checkbox"/> the name	<input checked="" type="checkbox"/> the address
<input type="checkbox"/> the nationality		
<input type="checkbox"/> the residence		
Name and Address DE VRIES, Johannes, Hendrik, Fokke De Vries & Metman B.V. Overschiestraat 180 NL-1062 XK Amsterdam Netherlands	State of Nationality	State of Residence
	Telephone No. 31 20 511 09 30	
	Facsimile No. 31 20 511 09 31	
	Teleprinter No.	
3. Further observations, if necessary:		
4. A copy of this notification has been sent to:		
<input checked="" type="checkbox"/> the receiving Office	<input type="checkbox"/> the designated Offices concerned	
<input type="checkbox"/> the International Searching Authority	<input checked="" type="checkbox"/> the elected Offices concerned	
<input checked="" type="checkbox"/> the International Preliminary Examining Authority	<input type="checkbox"/> other:	

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	Authorized officer Marie-José Devillard
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL PRELIMINARY EXAMINATION REPORT (PCT Rule 71.1)

To:	
DE VRIES, J.H.F. De VRIES & METMAN Gebouw Autumn Overschiestraat 184 N 1062 XK Amsterdam PAYS-BAS	
ingek.	04 FEB. 2000
dossier	WO 2585
termijn	
signaal	

Date of mailing (day/month/year)	02.02.2000
-------------------------------------	------------

Applicant's or agent's file reference WO 2585-dV/jdh	IMPORTANT NOTIFICATION :
---	---------------------------------

International application No. PCT/EP99/00283	International filing date (day/month/year) 14/01/1999	Priority date (day/month/year) 14/01/1998
---	--	--

Applicant MINDPORT B.V. et al.


1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.
2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.
3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. REMINDER

The applicant must enter the national phase before each elected Office by performing certain acts (filing translations and paying national fees) within 30 months from the priority date (or later in some Offices) (Article 39(1)) (see also the reminder sent by the International Bureau with Form PCT/IB/301).

Where a translation of the international application must be furnished to an elected Office, that translation must contain a translation of any annexes to the international preliminary examination report. It is the applicant's responsibility to prepare and furnish such translation directly to each elected Office concerned.

For further details on the applicable time limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Ahrens, R Tel. +49 89 2399-8730
--	--



09/600121

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference WO 2585-dV/jdh	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/EP 99/ 00283	International filing date (day/month/year) 14/01/1999	(Earliest) Priority Date (day/month/year) 14/01/1998
Applicant IRDETO B.V. et al.		

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of 3 sheets.



It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

- a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.



the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).

- b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing:



contained in the international application in written form.



filed together with the international application in computer readable form.



furnished subsequently to this Authority in written form.



furnished subsequently to this Authority in computer readable form.



the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.



the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished

2. ☐ **Certain claims were found unsearchable** (See Box I).

3. ☐ **Unity of invention is lacking** (see Box II).

4. With regard to the title,

the text is approved as submitted by the applicant.



the text has been established by this Authority to read as follows:

5. With regard to the abstract,

the text is approved as submitted by the applicant.



the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the drawings to be published with the abstract is Figure No.

as suggested by the applicant.



because the applicant failed to suggest a figure.



because this figure better characterizes the invention.

1

None of the figures.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference WO 2585-dV/jdh	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP99/00283	International filing date (day/month/year) 14/01/1999	Priority date (day/month/year) 14/01/1998
International Patent Classification (IPC) or national classification and IPC H04L29/06		
Applicant MINDPORT B.V. et al.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.



2. This REPORT consists of a total of 5 sheets, including this cover sheet.

☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of 2 sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☐ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 22/07/1999	Date of completion of this report 02.02.2000
Name and mailing address of the international preliminary examining authority:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Hamer, J Telephone No. +49 89 2399 8827 

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/EP99/00283

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

1-5 as originally filed

1a-1b as received on 12/01/2000 with letter of 12/01/2000

Claims, No.:

1-5 as originally filed

Drawings, sheets:

1/1 as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
☐ the claims, Nos.:
☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

**INTERNATIONAL PRELIMINARY
EXAMINATION REPORT**

International application No. PCT/EP99/00283

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-5
	No:	Claims	
Inventive step (IS)	Yes:	Claims	
	No:	Claims	1-5
Industrial applicability (IA)	Yes:	Claims	1-5
	No:	Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

V- Reasoned Statement

1. The following documents are cited:

D1: US-A-5 392 353 (MORALES FERNANDO) 21 February 1995
D2: US-A-5 432 850 (ROTHENBERG MICHAEL) 11 July 1995
D3: EP-A-0 808 048 (AT&T CORP.) 19 November 1997
D4: STALLINGS W: 'INTERNET ARMOR' BYTE, vol. 21, no. 12, December 1996, page 127/128, 130, 132, 134 XP000641459

2. The subject-matter of claim 1 is concerned with the secure transfer of data from a head end to a number of receivers. In order for the transmission to be secure, the transmitted data is scrambled and each receiver has a descrambler which requires a key to decrypt incoming data.

This kind of system is very well known in the art and forms the basis of most modern scrambled data transfer. In order for scrambled data to be transmitted, it is very obvious that the transmitter must possess a scrambler, and the receiver a descrambler with appropriate key.

The subject-matter of claim 1 further deals with how the receiver obtains its key. In claim 1, the key is sent to each receiver from the transmitter via the digital broadcast system. In the opinion of the examiner, it is an obvious measure to distribute the different keys. He is further of the opinion that, if the keys must be distributed, it is obvious to use the broadcast system. In fact, as the keys are required, the method of distributing them cannot be considered as involving an inventive step, whether they are distributed by courier, by post or over a broadcast network. Certainly in the case of claim 1, no surprising or inventive effect takes place.

As might be expected, the features of scrambled transmission and the descrambling thereof, and also the distribution of keys (also in an Internet environment) are found in the cited prior art documents (see passages cited in the international search report).

The applicant has argued that the difference between the subject-matter of the claims of the application and that of the prior art is that in claim 1, information intended for an individual receiver is supplied using a broadcast signal, whereas in documents D1 and D2, information is being sent point to point. This opinion is not shared by the examiner. It is true that in D1 or D2, a signal is supplied from an individual source, sent into the broadcast network and then can only be decrypted by an individual receiver. Taking only half of such a system, however, i.e. ignoring the source of the signal, one is left with a broadcast signal and an individual receiver which can decrypt the signal- just as in claim 1. Looked at alternatively, although signals in claim 1 are broadcast from a head end, in fact the signals intended only for an individual receiver must have an individual source. Thus, looked at one way, half of a system according to D1 or D2 is a broadcast system, or looking at claim 1 broadly but in the only way it can work, the system of claim 1 is a point to point system. Thus the aim and implementation of these systems is the same.

As the idea and the features of claim 1 are already well known and provide no surprising or inventive effect, claim 1 cannot be considered as involving an inventive step and does not therefore meet the requirements of Article 33(3) PCT.

2. Dependent claims 2 to 5 are not appended to an independent claim which meets the requirements of Article 33(3) PCT. Furthermore, their subject-matter does not appear to contain subject-matter which would add anything of inventive significance to that of claim 1. No features are disclosed which are not either already known from the prior art or which are not obvious to a person skilled in the art of transferring scrambled data

VII- Certain Defects

The following deficiencies are found in the application:

- a) The claims do not meet the requirements of Rule 6.2(b) PCT in that they do not contain reference signs.
- b) The independent claims do not meet the requirements of Rule 6.3(b) PCT in that they are not divided into the two-part form.

Page 1a

To be inserted on page 1, line 14

US-A-5 392 353 relates to an interactive satellite broadcast network, wherein encrypted communications ensure privacy of communications point-to-point in a network of interactive video stations interconnected by a broadcast network. Although a broadcast network is mentioned, this document refers to-point-point communications. Personal identification keys are used known only by the individual participating stations and a secure single central switching control center. The network control center intercepts communications encrypted as a function of the senders personal identification key and relays incoming communications designating the receiver in encrypted format as a function of the receivers personal identification key.

US-A-5 432 850 relates to a method and apparatus for secure data transmission, wherein a plurality of data frames are transmitted, each containing at least an encrypted data sequence employing the destination address as at least part of a decryption key. At the receiver side, the encrypted data sequence is decrypted by employing the local address of the receiver as at least part of the decryption key. In this known system each station can operate as a transmitting station using both the destination address and source address to encrypt the data.

EP-A-0 808 048 relates to a multimedia information service access, wherein a client can establish a connection with a server where desired multimedia information is resident. By selecting the desired multimedia information and providing a client information identifying the location of the user, the multimedia information is delivered by the server to a bridging

[16]

apparatus through a switched network. It is indicated that the delivery of the multimedia information can be secured by comparing the client information to a segmented list to determine whether the client is authorized to receive the requested multimedia information.

The article "Internet Armor" by W. Stallings, Byte, vol. 21, no. 12, December 1996, page 127-134, describes a method to provide secure IP package by encrypting the IP packet and providing a new IP header with the destination address.

10 This document however relates to transfer data through the Internet.



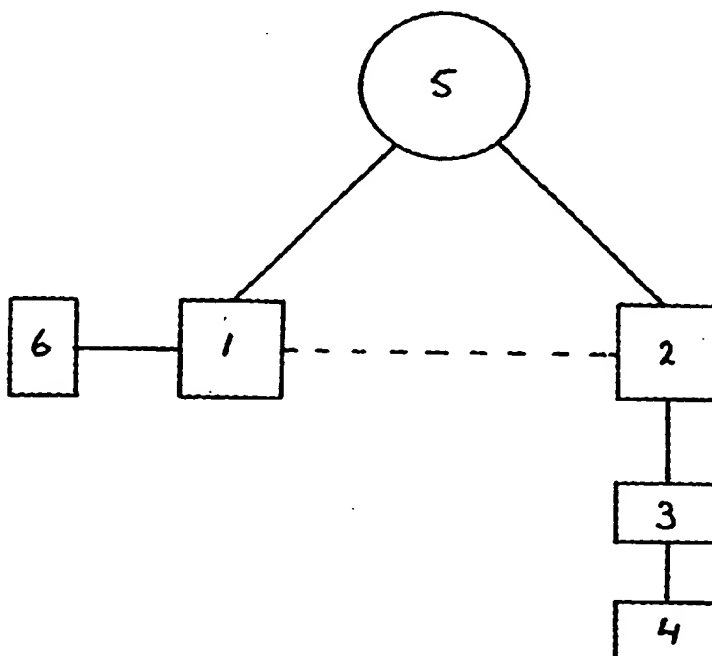
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification ⁶ : H04L 29/06		A1	(11) International Publication Number: WO 99/37069
			(43) International Publication Date: 22 July 1999 (22.07.99)
(21) International Application Number: PCT/EP99/00283 (22) International Filing Date: 14 January 1999 (14.01.99) (30) Priority Data: 98200081.2 14 January 1998 (14.01.98) EP (71) Applicant (for all designated States except US): IRDETO B.V. [NL/NL]; Jupiterstraat 42, NL-2132 HD Hoofddorp (NL). (72) Inventor; and (75) Inventor/Applicant (for US only): WAJS, Andrew, Augustine [GB/NL]; Schotersingel 93, NL-2023 AA Haarlem (NL). (74) Agents: DE VRIES, Johannes, Hendrik, Fokke et al.; De Vries & Metman B.V., Overschiestraat 184 N, NL-1062 XK Amsterdam (NL).		(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, ES, FI, FI (Utility model), GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG). Published <i>With international search report.</i> <i>Before the expiration of the time limit for amending the</i> <i>claims and to be republished in the event of the receipt of</i> <i>amendments.</i>	

(54) Title: METHOD FOR TRANSFERRING DATA FROM A HEAD-END TO A NUMBER OF RECEIVERS

(57) Abstract

A method for transferring data from a head-end to a number of receivers by means of a digital broadcast signal is described, wherein each of the receivers includes a descrambler for descrambling a received digital transport stream. The method includes sending a message from the head-end to each receiver to which data needs to be transferred. This message includes a key unique to the respective receiver and the unique key is loaded in the descrambler of the respective receiver. A table of unique keys with corresponding addresses of the respective receivers is provided at the head-end. Further at the request of at least one receiver, data packets with an individual address of this at least one receiver are provided and these data packets are inserted into transport packets of a digital transport stream. A key is selected from the table in accordance with the address of the data packet and the transport packets are scrambled using the selected key. The digital transport stream is broadcasted and received at one or more receivers. The scrambled transport packets of the digital transport stream are descrambled only at the receiver having the unique key used to scramble the scrambled transport packets.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakhstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Method for transferring data from a head-end to a number of receivers

The present invention relates to a method for transferring data from a head-end to a number of receivers by means of a digital broadcast signal, each of said receivers including a descrambler for descrambling a received digital transport stream.

The use of a digital broadcast signal, such as a DVB signal, for transferring data to one or more receivers shows the advantage that available receivers with descramblers can be used to transfer the data from a head-end to the receiver. However, such a method would normally not allow for a data transfer in a secure and private manner as the data is accessible to all receivers listening to the digital transport stream.

The present invention aims to provide a method of the above-mentioned type wherein privacy and security of the data transfer can be provided to each receiver.

According to the invention a method of the above-mentioned type is provided, including sending a message from the head-end to each receiver to which data needs to be transferred, said message including a key unique to the respective receiver, loading the unique key in the descrambler of the respective receiver, providing a table of unique keys with corresponding addresses of the respective receivers at the head-end, providing data packets with an individual address of at least one of said receivers, inserting said data packets into transport packets of a digital transport stream, selecting a key from said table in accordance with the address of the data packets, scrambling

said transport packets using the selected key, broadcasting the digital transport stream, receiving the digital transport stream at one or more receivers and descrambling the scrambled transport packets of the digital transport stream only at the receiver having the unique key used to scramble the scrambled transport packets.

In this manner a method is obtained wherein each receiver attempting to descramble the broadcast signal will fail to descramble the signal except for the receiver(s) having the unique key(s) used to scramble the transport packets in which the data packets are inserted which are intended to be received by this receiver. This results in the desired privacy and security for the data transfer between the head-end and the receiver.

In a preferred embodiment for transferring data packets to two or more receivers, the data packets for different receivers are inserted into different transport packets, each of said transport packets being scrambled with a unique key corresponding with the individual address of the corresponding data packets.

In this manner data transfer with privacy and security is provided for a number of receivers requesting the transfer of data.

The invention will be further explained by reference to the drawings in which an embodiment of the invention is schematically shown.

In this preferred embodiment the method is used to transfer data requested by a receiver from the Internet to the receiver on a digital broadcast signal or digital transport stream, so that an Internet connection is obtained with a high speed transfer of data to the receiver according to the Internet Protocol. However the method described can

also be used to transfer data to receivers at their request or initiated by the head-end in another manner.

In the drawing a DVB system is very schematically shown by way of example, the system comprising head-end
5 equipment 1 which will be indicated hereinafter by head-end, and a large number of subscribers having a receiver 2, only one of which is shown in the drawing. The receiver 2 includes a descrambler 3 co-operating with a smart card 4 in a usual manner. The descrambler 3 is used to descramble DVB services
10 requiring a subscription. The receiver 2 is connected to the Internet 5 in a manner not further shown, for example by a well-known modem. If the receiver 2 requests the download of data, the data will be transferred to the receiver 2 via the head-end 1 by means of a broadcast signal in the following
15 manner.

According to the internet protocol the data includes an IP or MAC address of the receiver 2 requesting the data to be transferred to this receiver. Each receiver 2 for which the head-end 1 receives data packets with an individual
20 address, i.e. the IP or MAC address, is sent a so-called Entitlement Control Message or ECM with a control word or key which is unique to the receiver 2. This message is encrypted using an individual key which is stored in the smart card 4. At the head-end 1 the unique keys with the corresponding
25 individual addresses are stored in a table 6. At the receiver(s) 2 to which an ECM is sent, the smart card 4 decrypts the received message using its individual key to obtain the unique key. The decrypted key is loaded into the descrambler 3 for future use.

30 At the head-end 1, the data packets for a specific receiver 2 requesting the transfer of data, are inserted into transport packets of the digital transport stream. Generally, the data packets are larger than the transport stream

packets, so that the data packets are split and thereafter inserted into a number of transport stream packets. Before scrambling the transport stream packets containing the data packets, the head-end checks the IP or MAC address and
5 selects the corresponding unique key from the table 6, which key is used to scramble the transport stream packets.

Each receiver 2 listening to the digital broadcast signal attempts to descramble the transport stream packets of the digital transport stream, wherein however only at the
10 receiver 2 having the unique key used for scrambling the transport stream packets, the descrambling process will be successful. In this manner only one receiver 2 will descramble the scrambled transport stream packets to thereby obtain the IP data packets.

15 From the above it will be clear that the described method results in a transfer of data with privacy and security for each receiver 2 requesting a data transfer. Moreover, this transfer with privacy and security is achieved while using existing DVB or MPEG scrambling and descrambling
20 equipment.

Generally, a number of receivers 2 will request the transfer of data. This is no problem as the head-end 1 will provide a table 6 including key/address combinations for each receiver 2 requesting a data transfer. The capacity of a
25 digital broadcast signal is sufficient to transfer IP data packets to a large number of receivers 2. As the IP data packets for each particular receiver will be inserted into a number of transport packets wherein only these transport packets are scrambled using the unique key for this particu-
30 lar receiver, data transfer will still take place in a private and secure manner.

The data packets can be inserted into transport stream packets of a digital transport stream which is used

for the transfer of data only. As an alternative the data packets can be inserted into transport stream packets of a DVB transport stream as the capacity of such a transport stream is far more than necessary for transferring the video
5 information.

Although in the preferred embodiment the method is used to transfer IP data packets, the described method can 5 also be used to transfer data from other sources than the Internet. Further, it is noted that instead of an ECM another
10 type of message may be used to transfer a unique key to a receiver.

CLAIMS

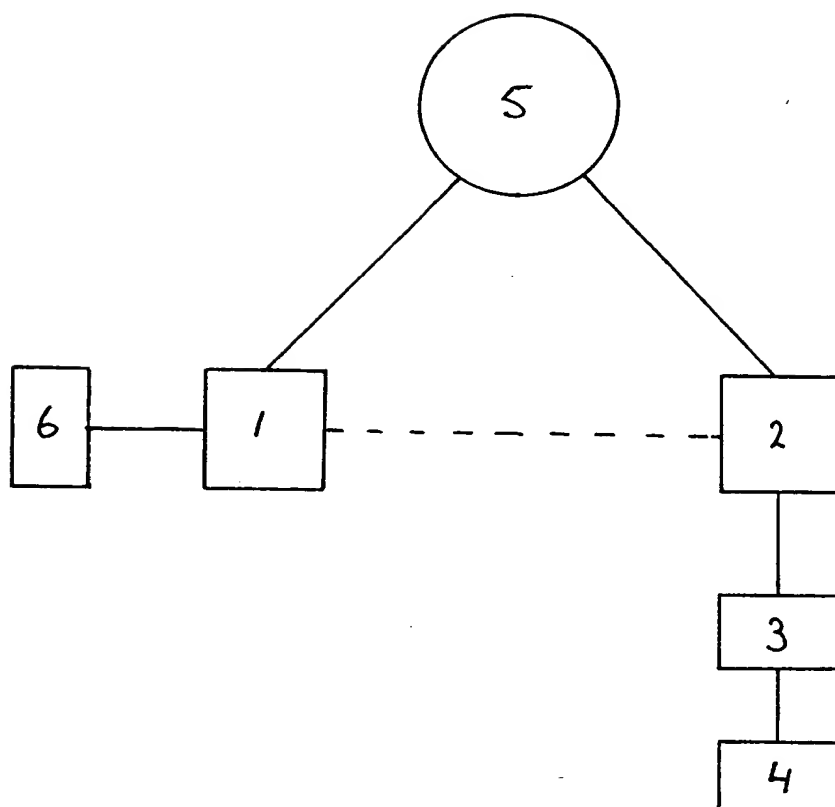
1. Method for transferring data from a head-end to a number of receivers by means of a digital broadcast signal, each of said receivers including a descrambler for descrambling a received digital transport stream, said method
5 including sending a message from the head-end to each receiver to which data needs to be transferred, said message including a key unique to the respective receiver, loading the unique key in the descrambler of the respective receiver, providing a table of unique keys with corresponding addresses
10 of the respective receivers at the head-end, providing data packets with an individual address of at least one of said receivers, inserting said data packets into transport packets of a digital transport stream, selecting a key from said table in accordance with the address of the data packets,
15 scrambling said transport packets using the selected key, broadcasting the digital transport stream, receiving the digital transport stream at one or more receivers and descrambling the scrambled transport packets of the digital transport stream only at the receiver having the unique key
20 used to scramble the scrambled transport packets.

2. Method according to claim 1, wherein for transferring data packets to two or more receivers, the data packets for different receivers are inserted into different transport packets, each of said transport packets being
25 scrambled with a unique key corresponding with the individual address of the corresponding data packets.

3. Method according to claim 1 or 2, wherein each receiver is adapted to request the transfer of specific data from the head-end.

4. Method according to claim 1, 2 or 3, wherein
5 the head-end and the receivers are connected to a network,
for example the internet, wherein one or more receivers
request the transfer of data from the network, wherein the
requested data together with the address of the requesting
receiver(s) is provided to the head-end in the form of data
10 packets and the head-end transfers the data packets to said
one or more receivers inserted in transport packets of the
digital broadcast stream.

5. Method according to any one of the preceding
claims, wherein the digital transport stream is a DVB
15 transport stream.



INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 99/00283

A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04L29/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5 392 353 A (MORALES FERNANDO) 21 February 1995 see abstract see column 2, line 36-51 see column 3, line 31-36 see column 4, line 25-30 see column 4, line 48-57 see claims 1,2,12 see figure 3 ---	1-4
Y	US 5 432 850 A (ROTHENBERG MICHAEL) 11 July 1995 see abstract see column 1, line 32-44 see column 2, line 9-24 see column 3, line 11-27 see column 4, line 8-12 see figures 1,3 ---	1-3

-/--

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
- "&" document member of the same patent family

Date of the actual completion of the international search

31 May 1999

Date of mailing of the international search report

15/06/1999

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Lázaro López, M.L.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 99/00283

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	<p>STALLINGS W: "INTERNET ARMOR" BYTE, vol. 21, no. 12, December 1996, page 127/128, 130, 132, 134 XP000641459 see column 4, line 36-45 see column 6, line 30-41 see column 7, line 22-27</p>	4
A	<p>EP 0 808 048 A (AT&T CORP.) 19 November 1997 see abstract</p>	4,5

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 99/00283

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5392353 A	21-02-1995	US 5663757 A	02-09-1997
		US 5101267 A	31-03-1992
		AU 634242 B	18-02-1993
		AU 5693790 A	20-12-1990
		CA 2018539 A	13-12-1990
		CN 1048136 A, B	26-12-1990
		CS 9002906 A	12-11-1991
		EP 0402809 A	19-12-1990
		JP 3064286 A	19-03-1991
		NO 176299 B	28-11-1994
		PT 94361 A	31-12-1997
		US 5257099 A	26-10-1993
		US 5223923 A	29-06-1993
US 5432850 A	11-07-1995	IL 102394 A	04-08-1996
EP 808048 A	19-11-1997	CA 2201999 A	15-11-1997
		JP 10107895 A	24-04-1998